REMARKS

Applicants request entry of the foregoing amendments to claims 1, 4, 13, 14, 15, 20, 23, 31, 32, 33, and 38.

Applicants are grateful to the Examiner for the telephone interview of June 2, 2005. In the interview, Applicants' representatives Ms. Wakimura and Mr. Wood, one of the inventors Dr. Gudbjartsson, and Examiner Klimach had a fruitful discussion. Two areas of claim amendments were identified that the parties felt would address the Examiner's concerns regarding the Spelman et al. reference.

The first area involved clarifying the sense in which the word "domain" is used in the claims, so that it cannot be confused with the use of the word "domain" as used in the phrase "domain name," where it is used to refer to different locations in a network.

To address this concern, applicants have amended the independent claims 1 and 20 so that they refer to a "working data identifier set domain." This language is intended to make clear that "domain," as used in the claims, relates to domains of sets of identifiers of working data, and not to locations in a network. Thus, for example, two different nodes or locations in a network might be in the same "working data identifier set domain," even though they are two different nodes in the network. In accordance with the discussion of the telephone interview of June 2, 2005, it is believed that this distinction helps to distinguish the Spelman et al. reference, as discussed further below.

The second area discussed in the telephone interview of June 2, 2005 involved clarifying that the phrase "identifier portion" in the claims referred to a data portion that identifies persons associated with the underlying research data, as opposed to identifying the sender or receiver of the working data. Thus, the independent claims have been amended to including the language that the working data includes "an identifier portion related to identifying persons associated with the research data portion."

In accordance with the discussion of the telephone interview, it is therefore believed that the rejections based on the Spelman et al. reference have been addressed.

Claims 1-4, 7-23, and 25-39 are rejected under 35 U.S.C. §103(a), due to either Spelman et al. alone, or a combination of Spelman et al. with Schneier, Ansell et al., or Coss et al.

Applicants submit that, as amended, independent claims 1 and 20 contain a number of important distinctions over Spelman et al., and are patentable over that reference. Applicants therefore respectfully request reconsideration and allowance of all remaining claims.

With reference to Fig. 1 of the Application, for the purposes of illustration, an example of the use of an embodiment according to the invention is to allow medical researchers to analyze large quantities of medical data collected from patients, without revealing the patients' identities to the researchers. For example, a data collector 109 that has a series of medical records containing both patient identifiers (such as their names and social security numbers) and research data about the patients (such as their blood pressures or cholesterol readings), may use an embodiment according to the invention to send the medical records to a data analyzer 110. Using the invention, the patient identifiers are made anonymous, such that the data analyzers 110 cannot make use of the patients' identities when analyzing the research data. However, the research data is left unmapped by the anonymous mapping of the patient identifiers, so that the data analyzers 110 can analyze the research data. Furthermore, the mapping itself between the data collector 109 and the data analyzers 110 is protected by requiring the data managers of the system that implements the mapping to use a secret sharing technique to control access to the mapping itself. This added protection of the mapping itself provides further security of patients' medical records.

By contrast, the basic use of Spelman et al. '445 is to allow a consumer 10 to order goods from a merchant 20. The merchant 20 obtains access to the consumer's goods and services order; and the merchant acquirer 40 (such as a bank) obtains access to the consumer's purchase instruction and credit card number. To allow this to happen properly, the merchant 20 communicates with a recryptor 30 that participates in a blinding protocol and validates the merchant and merchant acquirer (see Figs. 2A-2D).

One important difference of amended claims 1 and 20 over Spelman et al. involves the concept of communicating between different working data identifier set domains. There is a distinction between working data identifier set domains, on the one hand, and parties, on the other. In claim 1, as amended, it is required that the "apparatus [communicates] between parties comprising at least the sender and the receiver in at least two different working data identifier set domains." If Spelman et al. were to have the consumer 10 communicate with a merchant

acquirer 40 in a different working data identifier set domain, it would mean that the merchant acquirer 40 would not know the consumer's credit card number. This clearly is not the purpose of Spelman et al. – in fact the very opposite is true: Spelman et al. wishes to allow the credit card number to be known to both the consumer 10 and the merchant acquirer 40: they both must know the credit card number, and are therefore both in the same working data identifier set domain, even though they are different parties. Spelman et al. does not disclose or suggest communications between parties in different working data identifier set domains because such communications would be the direct opposite of what Spelman et al. is trying to accomplish: to actually allow the consumer 10 to get its personally identifiable credit card data through to the merchant acquirer 40. By contrast, Applicants' claims 1 and 20 are for preventing personal identifier data from getting through from a data collector to a data analyzer. Thus, applicants submit that claims 1 and 20 are neither disclosed nor suggested by Spelman et al. and are therefore patentable over that reference.

Another important difference between applicants' claims 1 and 20, as amended, and the Spelman et al. reference is found in the concept of anonymity. Claim 1, as amended, requires "anonymously mapping working data... [M]apping the identifier portion... such that the working data transmitted to the authorized receiver is anonymous data..." Method claim 20 contains analogous language. The system of Spelman et al. simply could not meet such claim language, because credit card transactions require the very opposite of anonymity: the merchant acquirer 40 (a bank) must know who the consumer 10 is, at least by some identifier; otherwise they would not know which account to debit for a purchase. The merchant acquirer 40 of Spelman et al. is therefore in a very different position from that of the data analyzer 110 of applicants' Fig. 1, because the data analyzer 110 receives "anonymous data," whereas the merchant acquirer 40 receives data that must be personalized. Because of this fundamentally different role, Spelman et al. does not disclose or suggest how to allow anonymous mapping of data. Thus, claims 1 and 20 are neither disclosed nor suggested by Spelman et al. and are therefore patentable over that reference.

Another important difference between the amended claims and Spelman et al. is that a system according to an embodiment of claim 1 communicates with two parties, whereas the recryptor 30 of Spelman et al. communicates with only one party – the merchant 20. This

difference is found in claim 1, as amended, in the language that states that "the apparatus [communicates] between parties comprising at least the sender and the receiver in at least two different working data identifier set domains." Analogous language is found in the first element of method claim 20. This language highlights the very different role that is played by the invention of applicants' claims 1 and 20 by comparison with Spelman et al. The recryptor 30 of Spelman et al. is used to communicate with only one party, the merchant 20, to participate in a blinding protocol and validate the merchant and merchant acquirer. By contrast, with reference to Fig. 1, the system 175 allows communication between the sender (such as data collector 109) and the receiver (such as data analyzer 110) in two different working data identifier set domains. Because of this fundamentally different role of communicating between two parties instead of with only one party, the recryptor 30 of Spelman et al. simply could not be used to accomplish the role required in claims 1 and 20, as amended; nor would such a role be suggested to one of ordinary skill in the art. Applicants therefore submit that claims 1 and 20 are neither disclosed nor suggested by Spelman et al. and are therefore patentable over that reference.

Another important distinction between the claims as amended and Spelman et al. is that recryptor 30 of Spelman et al. encrypts everything that it is sent (see Fig. 2C), whereas claim 1, as amended, requires "mapping the identifier portion... such that the working data transmitted to the authorized receiver is anonymous data, while leaving the research data portion unmapped by the anonymous mapping of the identifier portions." Method claim 20 contains analogous language. This language in claims 1 and 20, as amended, allows an embodiment according to the invention to perform an important function of applicants' invention: to allow researchers to analyze some of the data (the research portion), while keeping the rest of the data (the identifier portion) anonymous. The recryptor 30 of Spelman et al. could not perform this function because it encrypts all of the data that it sends back to the merchant (see Fig. 2C), as opposed to amended claims 1 and 20, which allow some of the data to be used as research data that is not mapped by the anonymous mapping of the identifier portions. Again, because of its fundamentally different role, the recryptor 30 of Spelman et al. simply could not be used to accomplish the role required in claims 1 and 20, as amended. Even if it were to communicate with more than one party (a distinction discussed above), the recryptor 30 would encrypt all of the data it was sent – even the research data that the analyzers would wish to access. A role such as that found in applicants'

claims 1 and 20 would therefore not be suggested to one of ordinary skill in the art. Thus, for this additional reason, claims 1 and 20 are neither disclosed nor suggested by Spelman et al. and are therefore patentable over that reference.

Another fundamental difference over Spelman et al. found in the language of claims 1 and 20 is that of secret sharing: claim 1 includes "a secret sharing module for performing secret sharing to control keyholder access to the mapping module." Method claim 20 includes similar language. There is no disclosure or suggestion in Spelman et al. of using secret sharing to control keyholder access to a mapping. A fundamental distinction is to be found between secure communications on the one hand, and access control to a mapping itself, on the other. In Spelman et al., there is a requirement of using digital signatures in the communications between the merchant 20 and the recryptor 30; but this only ensures secure communications between the parties. There is no disclosure or suggestion of techniques for access control to a mapping – for example, using secret sharing to control keyholder access to the mapping that is used to encrypt the data sent between the recryptor 30 and the merchant 20. The concept of secret sharing found in amended claims 1 and 20 relates to how data managers access a mapping, as opposed to how parties such as the recryptor 30 and merchant 20 ensure secure communications. Thus, for this additional reason, claims 1 and 20 are neither disclosed nor suggested by Spelman et al. and are therefore patentable over that reference.

Thus, Applicants' claims 1 and 20, as amended, involve different working data identifier set domains, anonymity, communications between multiple parties, selective anonymous mapping, and secret sharing; whereas Spelman et al. involves communication between parties in the same identifier domain, communicating a consumer's identity, allowing a recryptor to communicate only with one party (the merchant), and encryption of all data returned to the merchant. Independent claims 1 and 20 are therefore neither disclosed nor suggested by Spelman et al., and are patentable over that reference.

The remaining claims are all dependent on claims 1 and 20, and are therefore also allowable for the foregoing reasons. In addition, Schneier, Ansell et al., and Coss et al. do not add anything to the deficiencies of Spelman et al. discussed above, so that the various dependent claims are patentable over the combination of those references with Spelman et al.

CONCLUSION

In view of the above amendments and remarks, it is believed that all claims are in condition for allowance, and it is respectfully requested that the application be passed to issue. If the Examiner feels that a telephone conference would expedite prosecution of this case, the Examiner is invited to call the undersigned.

Respectfully submitted,

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

By 
Keith J. Wood
Registration No. 45,235
Telephone: (978) 341-0036
Facsimile: (978) 341-0136

Concord, MA 01742-9133
Dated: 6/6/05